UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/704,417	11/01/2000	Kenneth W. Aull	15-0231	4633

7590 04/20/2005

Christopher P. Harris
Tarolli, Sundheim, Covell & Tummino LLP
526 Superior Avenue
Suite 1111
Cleveland, OH 44114-1400

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/704,417	AULL, KENNETH W.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) *1-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The request for reconsideration file 11 March 2005 has been noted and made of record.

2. Claims 28-52 have been presented for examination.

Response to Arguments

3. Applicant's arguments filed 11 March 2005 have been fully considered but they are not persuasive.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. In response to Applicant's arguments that Ginter does not disclose or suggest authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate, the Examiner agrees. Ginter is cited to show an automated approach to obtaining a second certificate by using a first certificate. The last office action, as well as the current one, explicitly states that Ginter does not teach or disclose authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate.

6. In response to Applicant's arguments that Vogel does not disclose or suggest authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate, the Examiner disagrees. As the representative for Applicant points out on page 3 of the request for reconsideration, Vogel discloses authenticating based on multiple certificates. The examiner recognizes that obviousness can only be established

by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, there is a general knowledge readily available to those of ordinary skill in the art. At the time the present invention was made there was a general knowledge available to those of ordinary skill in the art of authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate. This is evident by U.S. Patent Nos. 5,922,074 (hereinafter '074) and 6,249,873 (hereinafter '873) which both state:

> If there is a valid certificate, the, in accordance with block **94** processing, the directory cross-references the client certificate, the server certificate and the communications context to retrieve an internally stored access control rule to apply to the client connection ('074, column 11, lines 21-25; '0873, column 11, lines 26-31).

The '074 and '873 patents establish that it was known by at least 13 July 1999 to check both a client and server certificate. This is further supported by U.S. Patent No. 5,659,616 (hereinafter '616) and U.S. Patent Application Publication 2002/0029337 (hereinafter '337), which state in the "Background of the Invention" that:

> Various security architectures define mechanisms to construct a certification path through the hierarchy to obtain a given user's certificate and all CA [certificate authority] certificates necessary to validate it ('616, column 3, lines 59-67; '337, page 2, paragraph [0015].

The '616 patent issued on 19 August 1997, thereby establishing that validating a user's certificate as well as its server certificate was well known as of that date. Therefore, authenticating based on multiple certificates is not over generalized, and one of ordinary skill in

the art would recognize the benefit of authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate.

7. As per the Applicant's arguments that Vogel does not disclose the obtainment of a second certificate, the Examiner agrees. Ginter was cited for teaching the automated obtainment of a second certificate in column 85, lines 11-15.

8. As per the Applicant's arguments that Moses does not recite sending a backup copy of the private key from the authority to a key recovery authority, the Examiner disagrees. The cited sections of Moses disclose:

> Another example of certificate option data may include data representing whether the certificate issuing unit 18 should generate the key pair and backup the corresponding private key at the certification authority for additional security.

If Moses' teaching of providing a backup copy of a private key to a key recovery authority, the Examiner asserts that it was well known at the time the invention was made. The Examiner asserts this allegation first with U.S. Patent No. 6,842,523 (hereinafter '523) which states at column 3, lines 48-57 that:

> This cryptographic communication system comprises a key recovery agent **3**, certificate authority **2**, and approver **4** to allow recovering a session key or user's private key in cryptographic communication communications between users **1*a*** and **1*b*.**

This at least establishes that has been well known in the art as the 102(e) date of the reference is 24 November 1999. U.S. Patent Nos. 6,549,626 (hereinafter '626) and 6,160,891 (hereinafter '891) also supports the Examiner's assertion in the "Background of the Invention" by stating in column 2, lines 33-41:

> To allow the recovery of a lost, forgotten or unavailable private key, some certificate authorities keep a copy of each private key in a vault or other form of key escrow.

Finally, in addition to the three prior references, U.S. Patent No. 6,389,136 (hereinafter '136) and 6,122,742 (hereinafter '742) states:

> This certificate of recoverability can be used to both recover the private key by the escrow authorities, and verify that the private key is recoverable ('136 and '742, column 2, lines 35-65).

Therefore, the Examiner believes it would have been well known to of ordinary skill in the art at the time the invention was made to have a backup copy of the private key at a key recovery authority.

9. See further rejections that follow.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 28, 35, 41, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6, 658,568 to Ginter et al., hereinafter Ginter, in view of U.S. Patent No. 6,816,900 to Vogel et al., hereinafter Vogel, and further in view of U.S. Patent No. 6,233,341 to Riggins, hereinafter Riggins.

12. As per claims 28, 35, 41 and 47, Ginter discloses a method for automatically obtaining a second certificate for a user using a first certificate, comprising:

accessing a registration server using the first certificate of the user to create a connection that authenticates the user's identity via the user's first certificate (Figure 51E [blocks 500a, 500b], column 85, lines 11-15);

forwarding a request for the second certificate from the user server to the registration server (column 85, lines 11-15);

determining in the registration server that the user is entitled to the second certificate (column 85, lines 11-15);

forwarding a request from the registration server to an authority (Figure 51E, column 86);

forwarding the second certificate from the another authority to a directory (Figure 52).

13. Ginter does not disclose authenticating both the user's server identity via a server certificate of the user serve and the user's identity via the user's first certificate;

creating a secure data channel between the registration server and the user server;

an authority to generate a private/public key pair;

sending the private key to the user from the authority via the secure data channel;

sending the public key from the authority to another authority to be signed.

14. Vogel discloses authenticating based on multiple certificates (column 4, lines 19-37); and creating a secure data connection (column 4, lines 19-37).

15. At the time the present invention was made there was a general knowledge available to those of ordinary skill in the art of authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate. This is evident by U.S. Patent Nos. 5,922,074 (hereinafter '074) and 6,249,873 (hereinafter '873) which both state:

> If there is a valid certificate, the, in accordance with block **94** processing, the directory cross-references the client certificate, the server certificate and the communications context to retrieve an internally stored access control rule to apply to the client connection ('074, column 11, lines 21-25; '0873, column 11, lines 26-31).

The '074 and '873 patents establish that it was known by at least 13 July 1999 to check both a client and server certificate. This is further supported by U.S. Patent No. 5,659,616 (hereinafter '616) and U.S. Patent Application Publication 2002/0029337 (hereinafter '337), which state in the "Background of the Invention" that:

> Various security architectures define mechanisms to construct a certification path through the hierarchy to obtain a given user's certificate and all CA [certificate authority] certificates necessary to validate it ('616, column 3, lines 59-67; '337, page 2, paragraph [0015].

The '616 patent issued on 19 August 1997, thereby establishing that validating a user's certificate as well as its server certificate was well known as of that date. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate based on multiple certificates and establish a secure connection therefrom, since Vogel states at column 4, lines 31-37 that such a modification deny access to users that could not verify the server identity thereby keeping malicious users from obtaining a certificate.

16. Riggins discloses an authority for generating a private/public key pair, sending the private key to the user, and signing the public key (column 1, lines 54-67).

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include an authority for generating a private/public key pair, sending the private key to the user, and signing the public key, since Riggins states at column 1, lines 40-53 that such a modification would utilize a well known and established method of recognizing entities participating in electronic transactions.

18. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins as applied above, in further view of U.S. Patent 6,108,788 to Moses et al., hereinafter Moses.

19. Regarding claim 29, Ginter, Vogel, and Riggins do not disclose sending a backup copy of the private key from the authority to a key recovery authority.

20. Moses discloses providing a backup copy of the private key (column 6, lines 1-14).

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to provide for a backup copy of the private key, since Moses discloses at column 6, lines 1-14 that such a modification would provide additional security.

22. Claims 30-34, 36-40, 42-46, and 48-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins as applied above, in further view of U.S. Patent 5,373,561 to Haber et al., hereinafter Haber.

23. Regarding claims 30, 36, 42, and 48, Ginter, Vogel and Riggins do not teach wherein the first certificate comprises a signature certificate.

24. Haber discloses a system for certifying or validating the existence or occurrence of a recorded document or event by relying upon cryptographic assumptions to establish the basis for such a certification or validation (col. 1, lines 6-10). Haber teaches extending the reliability of any type of certificate (i.e. signature certificate or encryption certificate) (col. 2, lines 51-54) by generating a new certificate from a combination of the original certificate and the original digital document (col. 2, lines 3-26).

25. Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Ginter and Riggins with the teachings of Haber to include that the first certificate comprises a signature certificate with the motivation to extend the validity of the original certificate (Haber col. 1, lines 53-56).

26. Regarding claims 31, 37, 43, and 49, Ginter, Vogel, and Riggins do not teach wherein the second certificate comprises an encryption certificate.

27. Haber teaches extending the reliability of any type of certificate (i.e. signature certificate or encryption certificate) (col. 2, lines 51-54) by generating a new certificate from a combination of the original certificate and the original digital document (col. 2, lines 3-26).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Ginter and Riggins with the teachings of Haber to include that the second certificate comprises an encryption certificate with the motivation to extend the validity of the original certificate (Haber col. 1, lines 53-56).

28. Regarding claims 32, 38, 44, and 50, Ginter, Vogel, and Riggins do not disclose wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

29. Haber teaches extending the reliability of any type of certificate (i.e. signature certificate or encryption certificate) (col. 2, lines 51-54) by generating a new certificate from a combination of the original certificate and the original digital document (col. 2, lines 3-26).

30. Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Ginter and Riggins with the teachings of Haber to include that the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate with the motivation to extend the validity of the original certificate (Haber col. 1, lines 53-56).

31. Regarding claims 33, 39, 45, and 51, Ginter, Vogel, and Riggins do not teach wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

32. Haber teaches extending the reliability of any type of certificate (i.e. signature certificate or encryption certificate) (col. 2, lines 51-54) by generating a new certificate from a combination of the original certificate and the original digital document (col. 2, lines 3-26).

33. Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Ginter and Riggins with the teachings of Haber to include that the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate with the motivation to extend the validity of the original certificate (Haber col. 1, lines 53-56).

34. Regarding claims 34, 40, 46, and 52, Ginter, Vogel, and Riggins do not teach wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

35. Haber teaches extending the reliability of any type of certificate (i.e. signature certificate or encryption certificate) (col. 2, lines 51-54) by generating a new certificate from a combination of the original certificate and the original digital document (col. 2, lines 3-26).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Ginter and Riggins with the teachings of Haber to include that the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption

certificate of the user with the motivation to extend the validity of the original certificate (Haber col. 1, lines 53-56).

Conclusion

36. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

37. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

40. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100